CLAIMS

1. A firewall (3), controlling network data packet traffic between internal and external networks (1,5,4), comprising filtering means, in dependence of the contents in data fields of a data packet being transmitted between said networks, selecting from a total set of rules a rule applicable to the data packet, whereby said packet is blocked or forwarded through the firewall (3), c h a r a c t e r i z e d by 2-dimensional address lookup means (8) performing a 2-dimensional lookup of the source and destination addresses of the packet in a set of address prefixes, each prefix having a subset of rules of the total set of rules, in order to find a prefix associated with said source and destination addresses, and rule matching means (10), performing - based on the contents of said data fields - a rule matching in order to find the rule applicable to the data packet.

2. A firewall according to claim 1, c h a r a c t e r i z e d by a fragmenting machine (11) fragmenting packets being too large to be handled and comprising fragment collecting means collecting packet fragments from a fragmented packet until a fragment header of said packet is received, fragment header storing means storing in an entry means information present in a fragment header field of the packet, fragment forwarding means forwarding packet fragments provided with fragment header information starting with the fragment header, wherein each fragment is processed by the filtering means as a regular unfragmented packet.

3. A firewall according to claim 1 or 2, c h a r a c t e r i z e d by network address translation means (12,14), translating in dependence of the information in the prefix internal source addresses to external source

addresses of a packet transmitted out through the firewall (3), or external source addresses to internal source addresses of a packet transmitted in through the firewall (3).

4. A firewall according to claim 1 or 2, c h a r a c t e r i z e d by network address translation means (12, 14), translating in depending of the information in the prefix internal source addresses to external source addresses of a packet transmitted from the internal network (1) to the external network (4), or external source addresses to internal source addresses of a packet transmitted from the external network (4) to the internal network (1).

5. A firewall according to any of the preceding claims, c h a r a c t e r i z e d by hole punching means (16,17), based on the information in the prefix determining if said packet is subject to a temporary exception from an external-to-internal blocking rule for a connection initiated from the internal network, wherein a return channel for packets transmitted from the external network (4) to the internal network (1) is established through the firewall during the lifetime of the connection.

6. A firewall (3), controlling network data packet traffic between internal and external networks (1,5,4), comprising filtering means, in dependence of the contents in data fields of a data packet being transmitted between said networks, selecting from a total set of rules a rule applicable to the data packet, whereby said packet is blocked or forwarded through the firewall (3), c h a r a c t e r i z e d by a fragmenting machine (11) fragmenting data packets being too large to be handled and comprising fragment collecting means collecting packet

fragments from a fragmented packet until a fragment header of said packet is received, fragment header storing means storing in an entry means information present in a fragment header field of the packet, fragment forwarding means forwarding packet fragments provided with fragment header information starting with the fragment header, wherein each fragment is processed by the filtering means as a regular unfragmented packet.

7. A method of controlling network data packet traffic between internal (1,5) and external networks (4) through a firewall (3), comprising the steps of,

in dependence of the contents in the data fields of a data packet being transmitted between said networks, selecting from a total set of rules a rule applicable to the data packet,

applying said rule on said packet,

and depending on the rule blocking or forwarding said packet through the firewall (3),

c h a r a c t e r i z e d in that said filtering comprises the further steps of:

performing a 2-dimensional lookup of the source and destination addresses of the packet in order to find a prefix associated with said source and destination addresses in a set of address prefixes, each prefix having a subset of rules of the total set of rules,

and based on the contents of said data fields of the packet, performing a rule matching on the subset of rules in order to find the rule applicable to the data packet.

8. A method according to claim 7,

c h a r a c t e r i z e d in that preceding the step of selecting a rule applicable to the data packet it comprises the further steps of:

collecting packet fragments from a fragmented packet until a fragment header of said packet is received,

storing in an entry means information present in a fragment header field of the packet, and

forwarding packet fragments provided with fragment header information starting with the fragment header, wherein each fragment is processed by the filtering means as a regular unfragmented packet.

9. A method according to claim 7 or 8, c h a r a c t e r i z e d in that preceding the step of performing a rule matching it comprises the further step of:

depending on the information in the prefix, translating the external source address to an internal source address of a packet to be transmitted in through the firewall (3).

10. A method according to any of the preceding claims 7-9, c h a r a c t e r i z e d in that preceding the step of performing a rule matching it comprises the further step of:

depending on the information in the prefix, translating the external source address to an internal source address of a packet to be transmitted from the external network (4) to the internal network (1,5).

11. A method according to to any of the preceding claims claims 7-10, c h a r a c t e r i z e d by the further step of:

depending on the information in the prefix translating the internal source address to an external source address of a packet to be transmitted out through the firewall (3).

12. A method according to any of the preceding claims 7-11, c h a r a c t e r i z e d by the further step of:

depending on the information in the prefix translating the internal source address to an external source address of a packet to be transmitted from the internal network (4) to the external network (1).

13. A method according to any of the preceding claims 7-12, c h a r a c t e r i z e d in that preceding the step of performing a rule matching it comprises the further steps of:

based on the information in the prefix, determining if said packet is subject to a temporary exception from an external-to-internal blocking rule for a connection initiated from the internal network (1),

if so, establishing a return channel for packets transmitted from the external network (4) to the internal network (1) through the firewall (3), having a duration corresponding to the lifetime of the connection.

14. A method of controlling network data packet traffic between internal and external networks (1,5,4) through a firewall (3), comprising the steps of,

in dependence of the contents in the data fields of a data packet being transmitted between said networks, selecting from a total set of rules a rule applicable to the data packet,

applying said rule on said packet,

and depending on the rule blocking or forwarding said packet through the firewall (3), c h a r a c t e r i z e d in that preceding the step of selecting a rule applicable to the data packet it comprises the further steps of:

collecting packet fragments from a fragmented packet until a fragment header of said packet is received,

storing in an entry means information present in a fragment header field of the packet, and

forwarding packet fragments provided with fragment header information starting with the fragment header, wherein each fragment is processed by the filtering means as a regular unfragmented packet.